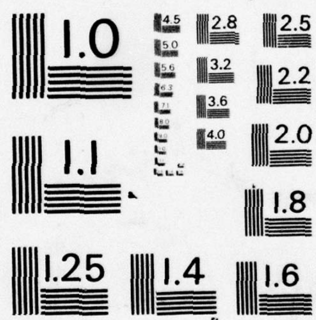
AD-A032 956 MITRE CORP BEDFORD MASS F/G 5/2
SECURE MULTILEVEL DATA BASE SYSTEM: DEMONSTRATION SCENARIOS.(U)
OCT 76 J L MACK, B N WAGNER F19628-76-C-0001
UNCLASSIFIED MTR-3160-VOL-2-REV-1 ESD-TR-76-158-VOL-2-REV-1 NL

1 OF 1
AD
A032956

END
DATE
FILMED
1 — 77



MICROCOPY RESOLUTION TEST CHART
NATIONAL BUREAU OF STANDARDS-1963-A

(12)

ESD-TR-76-158

MTR-3160, Vol. II
Rev. I

SECURE MULTILEVEL DATA BASE SYSTEM: DEMONSTRATION SCENARIOS

AD A 032956

OCTOBER 1976

Prepared for

DEPUTY FOR COMMAND AND MANAGEMENT SYSTEMS
ELECTRONIC SYSTEMS DIVISION
AIR FORCE SYSTEMS COMMAND
UNITED STATES AIR FORCE
Hanscom Air Force Base, Bedford, Massachusetts

Project No. 7070

Prepared by
THE MITRE CORPORATION
Bedford, Massachusetts
Contract No. F19628-76-C-0001

REVIEW AND APPROVAL

This technical report has been reviewed and is approved for publication.

Brian W. Woodruff

BRIAN W. WOODRUFF, 1Lt, USAF
Project Engineer

Lawrence A. Noble

LAWRENCE A. NOBLE, Major, USAF
Project Engineer

FOR THE COMMANDER

Stanley Paranka Col.

for: FRANK J. EMMA, Colonel, USAF
Director, Information Systems
Technology Applications Office
Deputy for Command & Management Systems

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

19 REPORT DOCUMENTATION PAGE		READ INSTRUCTIONS BEFORE COMPLETING FORM
1. REPORT NUMBER 18 ESD-TR-76-158-Vol-2-Rev-1	2. GOVT ACCESSION NO.	3. RECIPIENT'S CATALOG NUMBER
4. TITLE (and Subtitle) 6 SECURE MULTILEVEL DATA BASE SYSTEM: DEMONSTRATION SCENARIOS.		5. TYPE OF REPORT & PERIOD COVERED 14 MTR-3160-Vol-2-Rev-1
		6. PERFORMING ORG. REPORT NUMBER MTR-3160, Vol. II, Rev. I
7. AUTHOR(s) 10 J. L. Mack B. N. Wagner		8. CONTRACT OR GRANT NUMBER(s) 15 F19628-76-C-0001
9. PERFORMING ORGANIZATION NAME AND ADDRESS The MITRE Corporation Box 208, Bedford, MA 01730 12 49p.		10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS Project No. 7070
11. CONTROLLING OFFICE NAME AND ADDRESS Deputy for Command and Management Systems Electronic Systems Division, AFSC Hanscom Air Force Base, Bedford, MA 01731		12. REPORT DATE 11 Oct[redacted]76
		13. NUMBER OF PAGES 49
14. MONITORING AGENCY NAME & ADDRESS(if different from Controlling Office) 9 Technical rept.,		15. SECURITY CLASS. (of this report) UNCLASSIFIED
		15a. DECLASSIFICATION/DOWNGRADING SCHEDULE

16. DISTRIBUTION STATEMENT (of this Report)

Approved for public release; distribution unlimited.

17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)

18. SUPPLEMENTARY NOTES

19. KEY WORDS (Continue on reverse side if necessary and identify by block number)

AIR SURVEILLANCE
COMPUTER SECURITY
SCENARIOS
TEXT EDITING

20. ABSTRACT (Continue on reverse side if necessary and identify by block number)

The operation of a multilevel secure file management system using security kernel technology has been demonstrated under MITRE Project 7070. This volume of the project's final report describes three application scenarios used for demonstration of the system, and assesses their value and limitations.

DD FORM 1 JAN 73 1473 EDITION OF 1 NOV 65 IS OBSOLETE

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

235 050

ACKNOWLEDGMENT

This report has been prepared by The MITRE Corporation under Project No. 7070. The contract is sponsored by the Electronic Systems Division, Air Force Systems Command, Hanscom Air Force Base, Massachusetts.

TABLE OF CONTENTS

		Page
LIST OF ILLUSTRATIONS		4
SECTION I	INTRODUCTION	5
SECTION II	DEMONSTRATION OBJECTIVES	6
SECTION III	TEXT EDITING DEMONSTRATION	7
	APPLICATION SYSTEM CAPABILITIES	7
	ILLUSTRATIVE SCENARIO	9
SECTION IV	AIR SURVEILLANCE DEMONSTRATION	14
	PHYSICAL DESCRIPTION	14
	APPLICATION SYSTEM CAPABILITIES	16
	ILLUSTRATIVE SCENARIOS	16
	Southwest Scenario	17
	European Scenario	21
SECTION V	DEMONSTRATION ACCOMPLISHMENTS	26
	REPRESENTATIVENESS	26
	COMPLETENESS	27
	EFFECTIVENESS	27
SECTION VI	SUMMARY	30
APPENDIX I	LISTING OF TEXT EDITING SCENARIO WITH SYSTEM RESPONSES	31
APPENDIX II	SAMPLE TEXT EDITING PRINTOUT FROM LINE PRINTER AND DECWRITER	40
APPENDIX III	TRACK MESSAGE INPUT TIME LINES	42

LIST OF ILLUSTRATIONS

Figure Number		Page
1	Schematic Layout of Text Editing Demonstration - User #8 Logged on at Secret Level, User #9 at Unclassified Level	8
2	Data Block Structure of Sample Specification for Text Editing Scenario	10
3	Schematic Layout of Air Surveillance Demonstration	15
4	Southwest Air Surveillance Area with Aircraft Track Routes	18
5	European Air Surveillance Area with Aircraft Track Routes	22

SECTION I

INTRODUCTION

The automated near real-time handling of data from tactical sensors requires concurrent processing of data of various classification levels. In order to demonstrate the Security Kernel technology which can meet this need, a secure, multilevel, data base system has been developed under Project 7070, Secure Multilevel Data Base.

The focus of this project has been on the construction of a security kernel-based software system that will allow useful access to a multilevel data base. The system is capable of storing information from many sources of diverse classification and of allowing users at all clearance levels access to appropriate portions of that information. The users may operate concurrently on shared portions of the data base, so the system must provide sufficient support for shared access from different security levels, without compromising strict enforcement of security constraints.

One task of the project was the development of a scenario which requires the proposed multilevel data base system. This volume describes three scenarios for demonstration of the system; the first uses a text editing capability to show how a multilevel data base can allow data storage, manipulation and retrieval in a non-homogeneously-cleared user environment, while protecting all information from unauthorized access; the second is an Air Surveillance scenario which requires the addition of precisely controlled, selective downgrading of compartmented data, based on the informed judgment of a downgrading officer; and the third scenario, which presents a tactical air defense situation in Europe, also requires the downgrading and data base capabilities of the Air Surveillance system.

SECTION II

DEMONSTRATION OBJECTIVES

The overall objectives of the demonstration scenarios and tests are to demonstrate:

(a) that the kernel-controlled PDP-11/45 can effectively support a multiple security level data base system;

(b) that the system will protect classified information from security compromise;

(c) that the system can operate in an environment in which users with diverse clearance levels are performing concurrent operations on a data base with multiple levels of classified information; and

(d) that the system can support . secure downgrading facility suitable for a multi-source data correlation capability.

To meet these objectives we have developed two kinds of demonstration scenarios which are described in subsequent sections. These are:

(a) a Text Editing scenario to demonstrate that the kernel-controlled system can provide a capability for building and modifying a structured, multilevel data base which can serve a variety of users with differing clearances and needs-to-know, while constraining each user to access or modify only that data for which he is specifically authorized and cleared; and

(b) an Air Surveillance scenario that demonstrates, in addition, how the kernel-controlled system can be applied to correlate track data of differing classifications and can provide a facility for selective, controlled downgrading of classified information by the specific decision of an authorized downgrading officer.

SECTION III

TEXT EDITING DEMONSTRATION

The scenario for this demonstration illustrates a user's ability to access different levels of protected files through a text editor and utility exerciser. The text editor operates in the manner of most general system editors, its main purpose being to retrieve specified blocks of data and to perform simple manipulations on the data. The utility exerciser is used in the scenario as the means to change the discretionary file access rights of the particular user. In the demonstration, it is assumed that the user has acquired the "need-to-know" the contents of a specified file, and an operator gives him the corresponding access rights.

The secure file management system operates on the DEC PDP-11/45 minicomputer. The following peripherals are used in the demonstration:

(1) two Delta Data 5200 Video Display terminals, each with a dual-deck tape cassette drive,

(2) an LA30 DECwriter teleprinter, and

(3) a Centronics line printer.

The system assigns the two Delta Data displays to processes at security levels specified at user logon time. The attached tape cassette drive may be used to insert data into files through the editor. The DECwriter is assigned to the executive process, for use in allocation of the (variable security level) line printer. An operator uses the DECwriter to insure that the correct security level has been assigned to the line printer when a request to output information is made by an editor process. Figure 1 is a schematic layout of the system.

APPLICATION SYSTEM CAPABILITIES

Both the editor and the utility exerciser have commands which communicate with the Security Kernel of the file management system. The commands of the editor, as with many text editors, are concerned with creating or retrieving data files and with inserting, changing, or deleting data in the file. The security kernel insures that a user's files are protected against compromise.

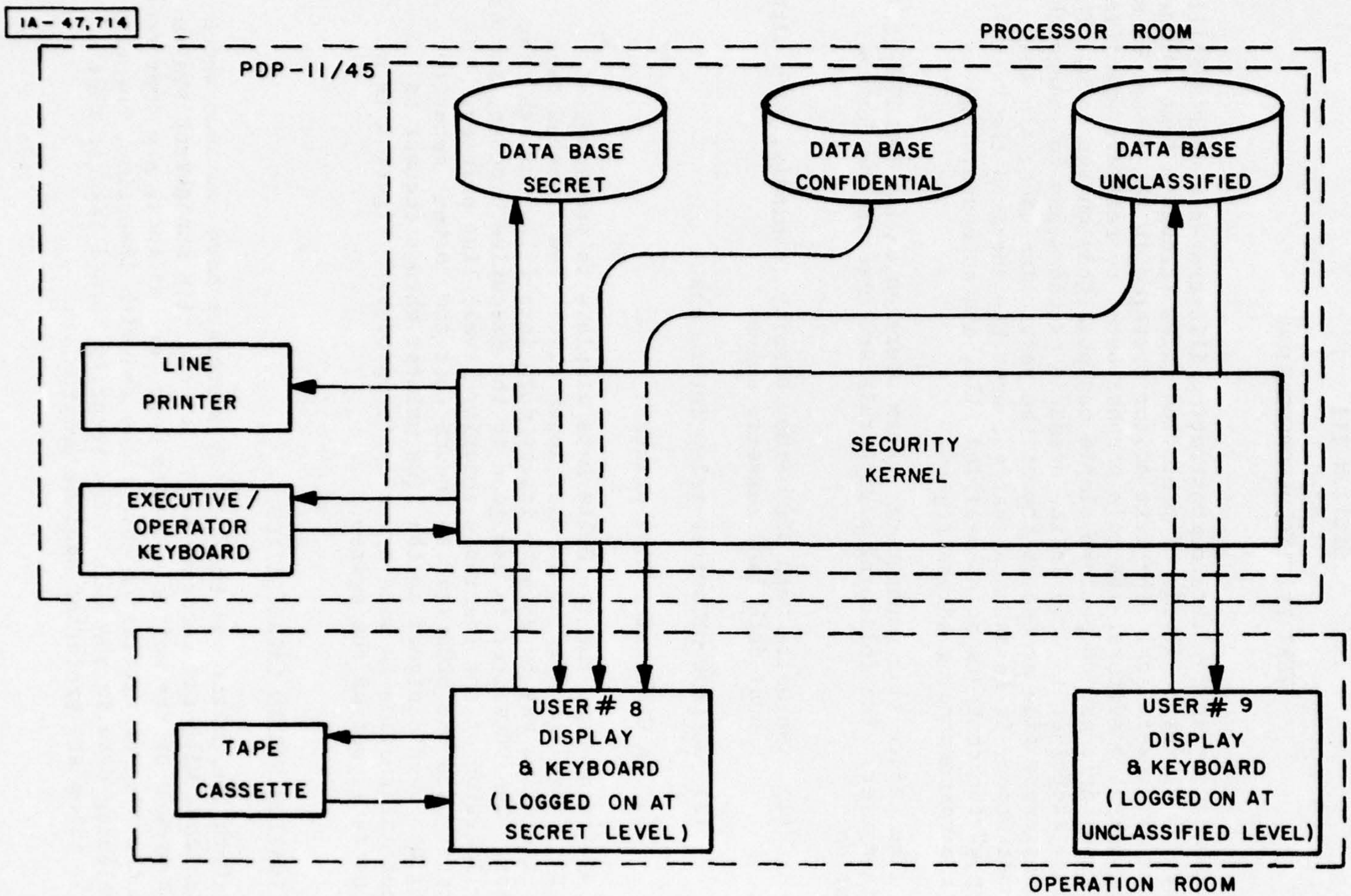


Figure 1. Schematic Layout of Text Editing Demonstration - User #8 Logged on at Secret Level, User #9 at Unclassified Level

The utility exerciser is used by a terminal operator to change the assigned access rights to specific files. Its main purpose is to give and rescind access rights, in order to exercise security kernel discretionary access capabilities.

The line printer program can be called from the editor, subject to the requirements of security protection. A user must be logged on to the system at the level of the highest classification of information that he wants printed; otherwise, no information is printed and an error message occurs. The system-high, trusted executive process, in conjunction with the kernel, handles the checking and starts the line printer process at the user's security level. The line printer process runs a modification of the editor program which analyzes the editor commands that fetch and print data files. These commands are stored by the user in a predefined block.

Another editor capability is the use of the tape cassette drive, attached to the Delta Data terminal, with the Insert command of the editor. Long data files, such as the one analyzed by the printer process, may be stored on a cassette tape and later inserted by the editor into the current block referenced by the user. The tape cassette may also be used to store sequences of editor commands.

ILLUSTRATIVE SCENARIO

The data on which the demonstration scenario operates are initially read into the system through use of the tape cassette. The tape contains the necessary system, editor, and utility commands to generate the environment. Through use of the Delta Data Control keys, blocks of information are read from the tape to the Delta Data memory, and each command or data line is then transmitted as a message to the system.

The blocks of data stored by the system, which may contain up to 15K bytes of information, are classified as either secret, confidential, or unclassified. These levels of classification were arbitrarily chosen for the demonstration; all information used therein is actually unclassified. Blocks are identified by a sequence of subscript numbers, which signify a block's position in the file tree relative to the root. A descriptive name for an immediately subordinate block may be associated with any subscript number, and this name may then be used in the identifying sequence instead of that subscript number. The descriptive name is arbitrarily chosen for user reference, to identify the information in the subsequent block. Figure 2 is a diagram of the block structure.

IA-46,989

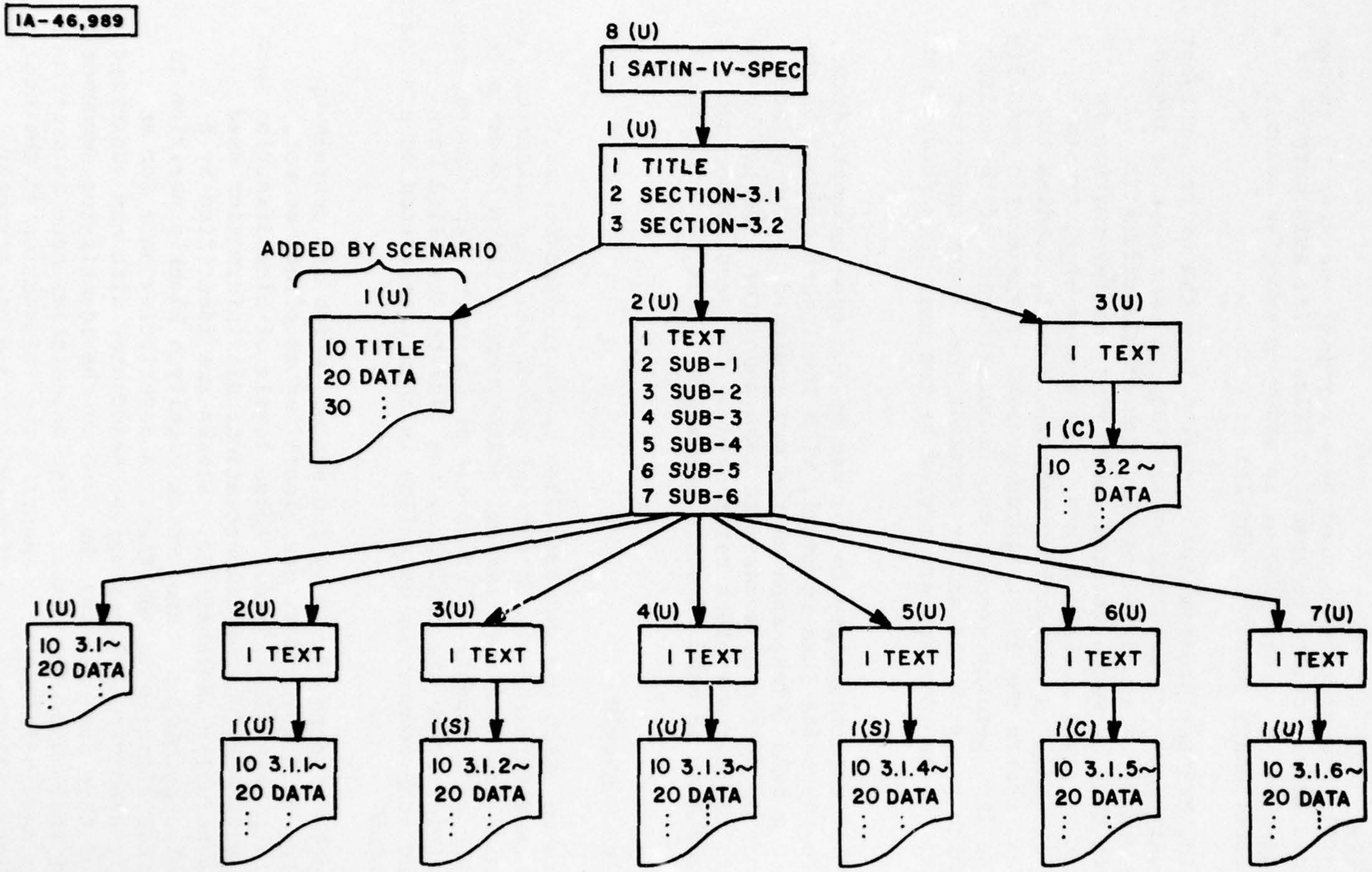


Figure 2. Data Block Structure of Sample Specification for Text Editing Scenario

In the scenario, two users operate on the system; they are referred to as User #8 and User #9. The file creation procedure gives User #9 write-read access to all of the blocks in User #8's structure except for the block nearest the root (block 8).

A brief explanation of the scenario session is given here. For further information, a detailed listing of the scenario with the system responses is contained in Appendix I. For the demonstration, an unclassified section of an early version of the SATIN IV System Specification was chosen as a text, and classifications were assigned to its various subsections. That particular text was chosen simply to provide a plausible illustration of the editor's application and does not imply any specific commitment on the part of SATIN IV.

In this demonstration, any user is allowed to logon at any console at whatever classification and category level he chooses. He is subject to the access rules for his chosen security level but is free to change his security level by logging off and back on the system. A system operating on genuine multilevel data would place bounds on the allowable process (and user) security levels, according to user identification or terminal location or both. These bounds would be under the control of a logon-user authentication program which is not incorporated into the system described here.

User #8 begins by logging on to the system under Project #2, at the unclassified level (U), with a category indicator of 0 (no categories). He first enters the editor. Two unclassified blocks are retrieved and listed on the display screen. User #8 then attempts to retrieve a confidential block of data, but the system responds that his access rights only extend through the unclassified blocks. File protection has been preserved. User #8 may advance only through the chain of unclassified blocks.

A new unclassified block is then added to the file structure. The title of the specification is inserted into this block. Another unclassified block is fetched from the block structure by User #8. Information is located and printed from the block. This confirms that read access does and should exist for the user. Character strings are referenced in the block and replaced by new data, thus illustrating the user's ability to write into the file.

User #8 now prepares to use the line printer. He logs off, and then on again at secret (S) classification, since the highest level of information to be printed is at the secret level. He enters the editor and fetches the block which is used to contain the printer commands. The Insert from Casette command is issued, which reads

the tape and stores the information into the current block. The user is now ready to request printing. Once the LP command is entered, a line printer process must be started at the user's current security level. The trusted executive process is the only process allowed (by the security kernel) to start a new process; it conducts a brief dialogue with the operator, via the DECwriter, to establish his cognizance of the printer's security level. Since the certified correct, trusted, executive process has exclusive control of the DECwriter, that device can supply an unforgeable record of the line printer process security level. The normal security kernel enforcement mechanism will insure that no information of higher security level is accessible to the line printer process; printout security markings applied or verified by the operator to be equal to the printer process security level are therefore guaranteed to be greater than or equal to the security level of the information printed. The questioning and response of the operator on the DECwriter and the eventual printout for the user are listed in Appendix II. The printout is prefaced and ended with an identifying page stating the user's process number. However, that process number cannot be guaranteed correct, because it could be "spoofed", or imitated, by a user level line print program. The checking of the operator's response at the DECwriter, on the other hand, is guaranteed to have been handled by the executive process, which is trustworthy.

User #8 then logs off, restarts at the unclassified level, and enters the utility program.

To illustrate a multi-user environment, User #9, at another terminal, has logged onto the file management system under project #2, at the unclassified level, with a category of 0. His purpose is to retrieve any of the files of User #8. Because User #9 does not have either write or read access to the first block in User #8's file structure, he is unable to achieve his goal. From the utility program, User #8 now gives User #9 write-read access to block 8 which, in turn, allows access to the rest of User #8's files, subject to the security level controls enforced by the kernel. This brief interchange simply illustrates the control of discretionary access between two users. At this point, observers of the demonstration are typically invited to logon to the system and exercise its text editing capabilities, in accordance with their own imaginations. Since access to data in the system is under the ultimate control of the security kernel, assurance that only proper access will be allowed is provided by confidence in the correctness of the kernel.

The purpose of the text editing scenario is to show the usability of a security kernel based system. Both terminals can edit a single copy of a file simultaneously, without any user awareness of the need to avoid interference, or of any time delays in the system's operation. Of course, no demonstration is adequate to assure the correctness of security controls; it simply provides an example of their effect on system operation under a specific set of circumstances.

SECTION IV

AIR SURVEILLANCE DEMONSTRATION

In this section we give a brief description of the air surveillance demonstration's physical arrangement; of the hardware and software capabilities and the displays and controls used to provide the man-machine interfaces; and finally, of the air surveillance demonstration scenarios.

PHYSICAL DESCRIPTION

All information in the Air Surveillance demonstration system is actually unclassified; for the purposes of demonstration, certain data is treated as though it were classified, intelligence information. The demonstration area is divided into two distinct parts which represent respectively, "intelligence" and "operations" areas. The simulated intelligence area includes a processor room, which houses the DEC PDP-11/45 minicomputer, supporting a security kernel-based file system of two different simulated security levels. An "intelligence" display and control room is also included in this area; there, an "intelligence" officer monitors an "intelligence" keyboard display and a downgrading display. The operations room contains an operations keyboard display operated by an Air Traffic Controller. Figure 3 illustrates the schematic layout of the demonstration system.

The processing of information involves two data bases in the file system: a compartmented data base and a collateral data base. The security kernel validates and controls access to these data bases, whether from internal operational processes or from the displays. The compartmented data base contains track information for use by the intelligence display and the downgrading display. The collateral data base can be read from all three displays: intelligence, downgrading, and operations.

The specific hardware used in the demonstration is the following:

(1) a DEC PDP-11/45 mimicomputer with memory management unit;

(2) an AN/FYQ-45 (BR-90) multi-function display console, which acts as the Air Situation Monitoring Console (intelligence display);

IA-46,928

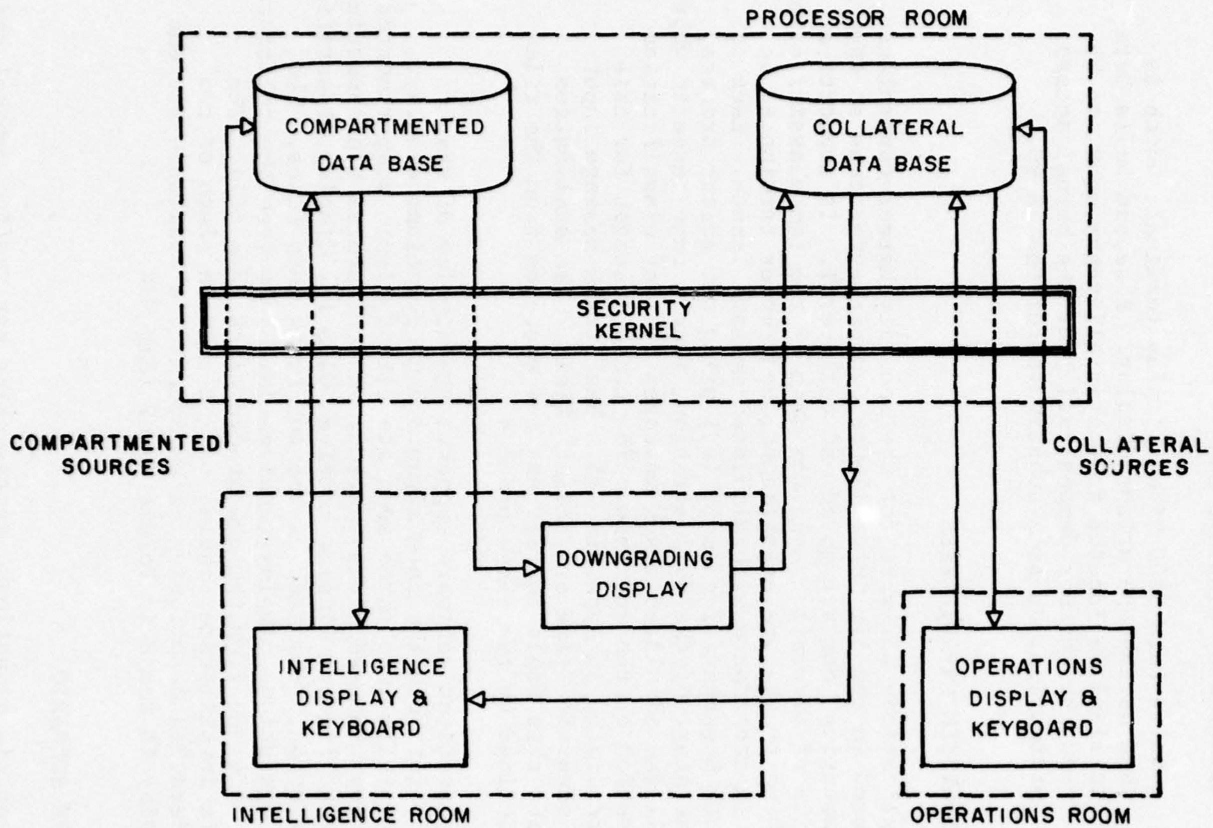


Figure 3. Schematic Layout of Air Surveillance Demonstration

(3) an ASR-33 teletype, which fills the role of the downgrading display; and

(4) a Delta Data 5200 Video Display terminal, which is used as the operations display. A second Delta Data terminal is located in the intelligence room, to be used for further demonstration of the kernel access protection, or as a substitute for the BR-90.

APPLICATION SYSTEM CAPABILITIES

The applications software for the security kernel-controlled PDP-11/45 used in the Air Surveillance demonstration runs at two levels of security, compartmented and collateral. It supports a separate file of aircraft tracks for each of the two classification levels. These tracks are established, updated or terminated in the system in accordance with simulated message inputs. Each of the two track message files is filled, using the editor process, prior to the start of the demonstration, from a tape cassette which contains all the simulated track messages of that classification for the duration of the scenario. The track messages for this scenario are listed in Appendix III. Each track message input contains a scenario "time of receipt" field. The application software uses this field to retrieve the messages from the files at a time defined by the clock process.

The applications software supports the display of track information, for both the intelligence and operations display. This support falls into three separate cateogories: compartmented graphics, compartmented alphanumerics, and collateral alphanumerics. The BR-90 intelligence display receives data for display, identified by classification, from each of the two track data files. The collateral operations display receives data only from the collateral track data file and from the downgraded track data file. The alphanumeric intelligence display can be used in place of the BR-90. A detailed description of an operator's available actions at the display is found in Volume IV of this MTR.

ILLUSTRATIVE SCENARIO

Two scenario situations, representing air traffic control and tactical air defense, were developed to illustrate the multilevel air surveillance/monitoring concept. Both scenarios feature two levels of user simulation information sensitivity, two corresponding levels of user access authorization, and a requirement for controlled, selective downgrading of compartmented data by a cleared person in

order to provide a collateral-level Operations Controller with enough information to warn him of potentially hazardous or threatening tracks.

The air surveillance scenarios are identified by the location of their converage areas: the Southwest scenario, which involves the southwestern United States, and the European scenario, which concerns the border separating the Federal Republic of Germany from East Germany. The Southwest scenario has an Air Traffic Controller monitoring civilian and military aircraft around a restricted use air space; the European scenario illustrates the monitoring of aircraft performing tactical maneuvers along the East/West border. The following subsections give detailed descriptions of each scenario regarding the situation, setting, action overview, and user/system interaction.

Southwest Scenario

Situation and Setting

The scenario setting is in the southwestern United States. An Air Surveillance and Control System (ASCS) located in that area has coverage of the area bounded by 103 and 109 degrees west longitude, and by 31 and 35 degrees north latitude. This coverage area is shown in Figure 4. The paths of the aircraft tracks followed in the scenario are also included on the map.

The ASCS receives air track report messages from six sensor sources. The information about the location, characteristics, and track reports of four of these sensors is collateral information. Information about the existence, location, characteristics, and track reports from the other two sensors is compartmented information. These latter two sensors are located within a large, irregularly shaped "Restricted Use Airspace" (RUA) which occupies an area near the center of the ASCS coverage. Track reports of air activity within the RUA are received solely from the two sensitive sources. All tracks which originate or are contained within the RUA are tentatively assigned a high classification. All other tracks are reported by the collateral-level sensors and are themselves collateral data.

The ASCS is the primary source of data for surveillance and control of the airspace in its area of coverage. It is the only source of track data to the Air Traffic Controllers who are responsible for maintaining safe flight path separations between all the aircraft in the area. The existence of the classified RUA in the center of the area causes a conflicting set of data and security management requirements. The Air Traffic Controller needs adequate data on all tracks to support his prevention of potentially hazardous flight path interference, yet the security regulations

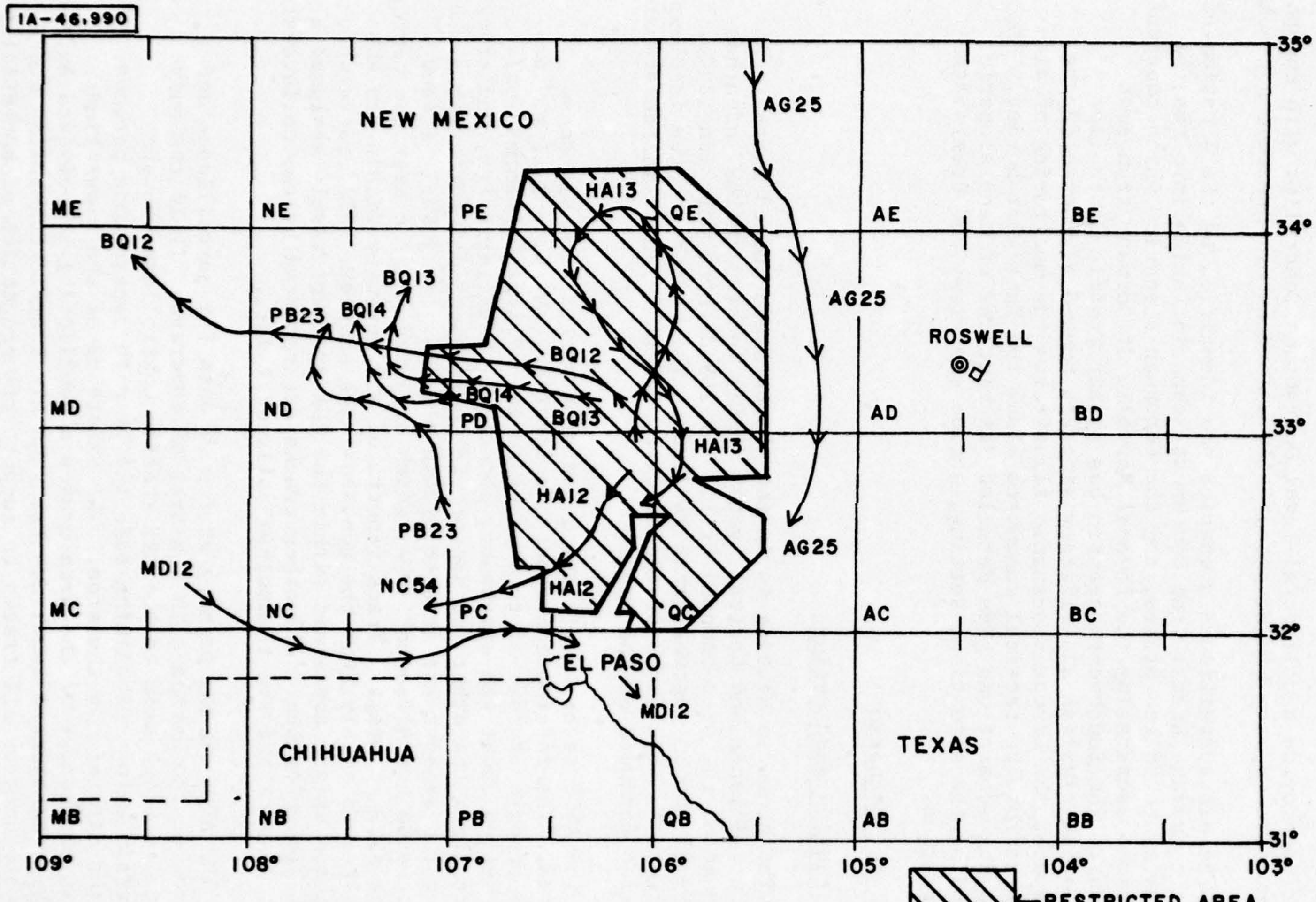


Figure 4. Air Surveillance Area with Aircraft Track Routes

require that the compartmented tracks and their sources not be divulged to the Air Traffic Controller, because he and his operating area are not cleared for this information. These opposing requirements are resolved by the use of a multilevel secure system.

The responsibility for monitoring compartmented and collateral tracks, and for determining when a potential for hazardous flight path interference exists between compartmented and collateral tracks, is placed on the cleared Air Surveillance Monitoring/Downgrading Officer (ASM/DO). The ASM/DO operates at the Air Surveillance Monitoring and Control Console (the BR-90) and the adjacent Downgrading Teletype Terminal (ASR-33). The ASM/DO monitors the graphic display of the BR-90, using the lightgun and variable function keys to aid his monitoring. He can select tracks for special alphanumeric track displays on the BR-90. If, in the judgment of the ASM/DO, any of the compartmented-level tracks appear to constitute a potential hazard to flight safety with a collateral track, he prepares to make a downgrading decision.

When the ASM/DO decides that data on the compartmented track should be downgraded, he lightguns its track symbol on the graphic display and depresses the function key labeled "PASS". These actions will cause the downgrading of the current track parameters (TRN, Position, Heading, Speed, Altitude), which are passed to the ASR-33 teletype Downgrading Console. A hard copy is produced at the ASM-33 as a guaranteed record of the downgraded tracks. The downgraded track data, shown on the ASR-33 and stored in the downgrading file, is then passed to the collateral track file and displayed in the special attention area of the collateral Air Traffic Controller's display. The classified Track Reference Number and source identity are not passed for downgrading due to the selected downgrading parameters used for the demonstration system. The information to be downgraded is selected and formatted by uncertified software, but the hard copy record provides the critical certified audit of downgraded information.

The downgraded track parameters are a snapshot of the track at the moment of the downgrading request decision at the BR-90. The downgraded track is entered as a new track to the collateral track file, and then will be updated by a simple extrapolation of the specific downgraded data. No further updating of the track using compartmented data will occur unless an update decision is made by the ASM/DO. When an update downgrading is performed by the downgrading officer, the update message is printed on the ASR-33 and passed to the downgraded file. The low-level process enters the message as a one-time update of the collateral track file; extrapolation of the updated data at the low level is then continued.

Action Overview

The duration of the scenario action is 20 minutes. The number of active tracks in the system varies from three to eight. Two potential conflict situations occur between compartmented "test" aircraft tracks and collateral-level tracks. In one case the potential track conflict is with a general aviation aircraft. In the other case it occurs with the track projection of a non-military U.S. Government aircraft. In both situations, the course and flight parameters of the compartmented track are downgraded, and the collateral track alters course to indicate response to the Air Traffic Controller's instructions. We demonstrate that the Air Traffic Controller can only obtain compartmented data which has been downgraded. In a third situation, a "company executive" aircraft leaves the RUA without a potential flight path conflict; multiple trackings occur from both levels of sensors until the ASM/DO determines that the tracks are the same aircraft and pairs them together.

Scenario Interaction

A more detailed description of certain track interactions is presented as viewed by the ASM/DO. Referring back to Figure 4 will help in following the discussion.

Within the first four minutes of the scenario, four compartmented tracks (HA12, HA13, BQ12, BQ13) have appeared on the BR-90 display and their courses are extrapolated. Three collateral tracks (MD12, PB23, AG25) have also entered the area. Four minutes later, it becomes apparent the PB25, a general aviation aircraft, may interfere with the compartmented track, BQ13. At this point, the ASM/DO downgrades BQ13 by lightgunning the track, pressing the PASS button, and afterwards, on the teletype, accepting the downgraded message. At eleven minutes into the scenario, a compartmented aircraft (BQ14) splits off from track BQ13, since two tracks make up track BQ13. The ASM/DO then decides to update the information concerning track BQ13 at the low display. He lightguns BQ13 and issues the UPD for that track.

Two minutes later a general aviation aircraft (NC54) is recorded by a collateral-level sensor and appears on the display. This track seems to have the same tracking data as HA12, so the ASM/DO continues to monitor it.

At fifteen minutes into the scenario, the ASM/DO concludes that HA12 and NC54 are, in fact, the same track being recorded by both levels of sensors. He performs an ASSOCiate on the two tracks to clear the display of the multiple tracking. The ASM/DO also decides that the operations controller no longer needs information about BQ13 so the downgraded collateral track is deleted by a TERMinate action. A record of this action also appears on the teletype for verification.

At this point in the demonstration, attention is centered on the operations display. From the intelligence display a compartmented track, HA13, is downgraded and the resulting new collateral track is observed in the special attention area of the operations display. The downgraded track also appears in the track file. Later, this track is TERMinated by the ASM/DO. The operations controller is notified in the special display area and the track is deleted from the collateral file.

As the scenario continues, the access protection of the scenario files is demonstrated by entering the text editor from either the operations display/keyboard or the intelligence display/keyboard. Depending on the designated classification of each data block, files are successfully retrieved or access is denied.

European Scenario

Situation and Setting

The scenario setting is the area on both sides of the East-West German border. The Air Surveillance and Control System (ASCS) in the area has coverage bounded by 8 degrees and 16 degrees east longitude and by 50 degrees 40 minutes and 54 degrees north latitude. The West German area is called Blueland; East Germany and contiguous regions of the Warsaw pack countries are Redland. The projection slide for the BR-90 has these areas outlined by separate colors: green for the geographic limits of Blueland and red for the areas of Redland outside the coverage of the Blueland operations surveillance system. A third area, outlined in yellow, designates the coverage in Redland of the radars, located in Blueland, which feed track data to the Blueland operations surveillance system. The slide includes a "never downgrade" contour in Redland, east of which tracks should never be downgraded. This contour closely parallels the border of Poland. The three flight access corridors from West Germany to Berlin are also marked on the slide. The slide map with aircraft tracks is illustrated in Figure 5.

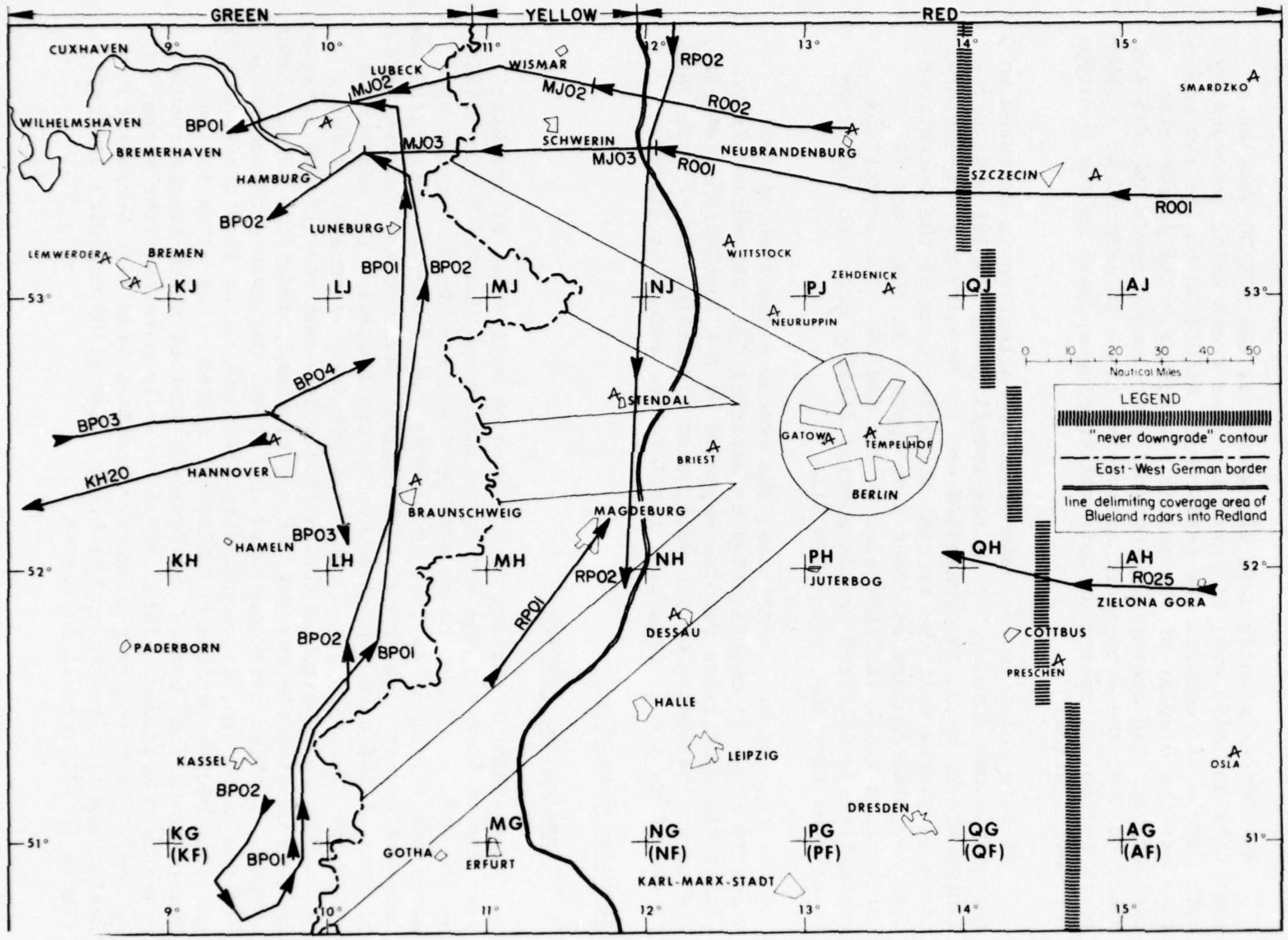


Figure 5. European Air Surveillance Area with Aircraft Track Routes

The ASCS receives track reports from sensor sources in the three areas designated on the slide map. Collateral tracks are reported to the Blueland operations surveillance system only from radars located in Blueland. Their coverage area includes all the territory within Blueland plus that area of Redland covered by the Blueland radars near the border. The green and yellow areas of the map coincide with the aforementioned coverage areas. Compartmented track information is reported by intelligence sources and facilities from the red area of the map. The location, characteristics, and existence of these sources are assumed to be special access classified intelligence information. This intelligence track data may be made available to Blueland operations only by intelligence downgrading decisions.

The monitoring of both compartmented and collateral tracks is done by the Air Surveillance Monitoring/Downgrading Officer (ASM/DO). The ASM/DO also determines when a potential threat situation exists from tracks in the compartmented data base. When he makes a downgrading decision, the flight information of the compartmented track is stored in the downgrading file and then passed to the collateral track file of the operations controller. The information is displayed in the special attention area of the operations display. A hard copy of the downgraded track message is printed on the ASR-33. The ASM/DO is not required to acknowledge the downgraded message printed at the teletype. For the demonstration scenario situation, a high level of alert is assumed. In this circumstance, the ASM/DO will always downgrade a track as soon as it crosses the "never downgrade" line.

Action Overview

The scenario begins with Redland and Blueland patrol aircraft maintaining air coverage in a "race track" flight pattern along their respective sides of the East/West border. Threat situations occur at two different times in the scenario when attack aircraft from the East threaten to cross the border into Blueland. In both cases, the ASM/DO conveys the potential threat to the operations console by downgrading the compartmented track data. The collateral Operations Flight Controller sees the potential threat situation and can alert the Blueland patrol aircraft to react to it. In both situations, the Redland threat aircraft cross the border, and the Blueland patrol aircraft successfully intercept the penetrators. The scenario action occupies twenty minutes, and the number of active tracks in the system varies from four to seven.

Scenario Interaction

A tracing of the aircraft tracks is presented to better illustrate the movement/engagement of aricraft during the scenario. Referring back to Figure 5 will help in following the discussion.

The beginning layout of tracks is on the BR-90 display screen shows three types of aircraft. A commercial aircraft (KH20) is heading southwest at a low altitude after taking off from the Hanover area. Two flights of Blueland patrol aircraft (BP01, BP02) appear near the bottom of the screen and commence a race track flight pattern closely paralleling the border with one patrol heading north and the other heading south. A Redland aircraft (RP01) is also patrolling the area between Berlin and the border.

Two minutes into the scenario, the threat aricraft from the East enter the arena north of Berlin. First, the intelligence track (R001), consisting of three aircraft from Redland, appears in the "never downgrade" area. A minute later, another intelligence track (R002) appears west of the "never downgrade" contour. The intelligence officer identifies the type of aircraft (military), analyzes the direction of the aircraft's flight, and decides that a potential threat exists. He then downgrades the track in order to give the operations officer early warning about the flight path and size of the potential threat aircraft track. The downgrade track (Z001) now appears on the screen. For the purpose of improving legibility on the BR-90 screen, the intelligence operator turns off the symbology for the downgraded track.

Another Redland patrol (RP02) appears at the top of the BR-90 screen after the downgrading procedure is completed. A minute later, the intelligence officer updates the downgraded flight information for track R002. As the Blueland patrol (BP01) is notified by operations of the potential threat situation, the track for BP01 increases speed to close with track R002's predicted flight path, for potential defensive action.

At seven minutes into the scenario, track RP01 has crossed the "never downgrade" line. The intelligence officer notes that the three military aircraft track, R001, is heading in the direction of the border, and he downgrades the track information (downgraded track number Z002). Soon after this downgrading has occurred, R001 changes its heading; consequently the downgraded track information for Z002 no longer accurately represents the current position and heading of R001. The downgrading officer updates the downgraded track. Another Blueland patrol (BP02) is diverted from patrolling the border and heads north toward the potential conflicts.

When the Red aircraft (R002) enters the coverage area of Blueland radar (yellow area on screen), its unclassified radar track (MJ02) enters the collateral data base and appears on both the intelligence and operations displays. The downgraded track (Z001), associated with Red aircraft R002, is terminated, because it appears on both

displays and is no longer needed. The intelligence track (R002) also disappears because the operations officer has the low level track MJ02 on his display. Track MJ02 is identified and followed as the threat aircraft.

During this period, the Blueland patrol (BP01) is closing the distance to the potential penetrator MJ02. The Redland patrols are continuing their surveillance. After eleven minutes, a Blueland patrol force replenishment track (BP03) appears from the west edge of the BR-90 screen.

At thirteen minutes into the scenario, track R001 reaches Blueland radar coverage and receives a collateral track identifier (MJ03). The downgraded track (Z002) is terminated and R001 is also deleted from the screen. At this time, the Redland aircraft (MJ02) crosses the border into Blueland, and the Blueland patrol aircraft (BP01) engages the penetrator. A minute later, track MJ02 disappears from the display. The Blueland patrol replenishment track (BP03) comprised of "many" aircraft splits into two tracks (BP03, BP04). Each is headed for a different section of the patrol race track.

At sixteen minutes into the scenario, BP02 engages MJ03 at the border and threat track MJ03 is neutralized. Both threat situations have now been eliminated.

Two minutes later, a new intelligence track (R025) appears in the "never downgrade" area. This track will be downgraded for the purpose of demonstrating the type of downgraded information that is passed and displayed to the operations controller. The result will be that a new collateral track (Z003) appears in the special attention area of the operations display and also in the track file of operations. The downgraded track (Z003) can also be updated resulting in an updated message appearing in the special attention area of the operations display. The information in the operations track file is also changed to reflect the update operation.

As with the air traffic control scenario, the access protection of the scenario files can be demonstrated by entering the text editor from either the operations display/keyboard or the intelligence display/keyboard.

SECTION V

DEMONSTRATION ACCOMPLISHMENTS

In this section, the degree to which the scenarios described in the previous sections achieve the intended objectives of the demonstration will be examined. The examination will cover three broad areas: the representativeness of the scenarios in modeling Air Force needs and applications, particularly with regard to multi-source correlation; the completeness of the scenarios insofar as they demonstrate the use of and need for each of the features of the software system; and the effectiveness of the scenarios in demonstrating the capability of a multilevel secure data base system with a controlled downgrading facility.

REPRESENTATIVENESS

The two types of scenarios described herein are, with a minimum of abstraction, representative of actual Air Force applications. The text editing demonstration is an example of a system in which textual or other data base information is maintained on a computer for access by a variety of users. In a system of this nature, where the stored data is a mixture of information of various classifications, the ability to operate in a multilevel secure manner is advantageous from a cost and effectiveness point of view. In the absence of a multilevel secure capability, the principal alternatives are: (a) to store all the information at the highest security level, rendering even unclassified information inaccessible to users without the highest clearances, (b) to store the various security levels of information separately in either space (different systems) or time (color-changing), so that concurrent access to information of more than one security level is impossible, or (c) to add to the second alternative the storage of multiple variously-classified copies of the information actually of lower security levels, making concurrent access possible but adding the complexity and lack of consistency inherent in storing information independently in a variety of repositories. Each of these alternatives imposes cost and operational constraints which may not be acceptable in a given system.

The Air Surveillance scenario is representative of a more complex system in which time-critical operations are inherent in the system's mission. In the environment of the Air Surveillance demonstration, the time-critical factor is a product of potential interference between the flight paths of two friendly aircraft. In

another environment, the time-critical element might be impending conflict with an unfriendly aircraft, or the possible approach of an unidentified target. In each of these circumstances, response time is a fundamental characteristic of the system, imposed by external requirements rather than by operational convenience or cost limitations. The need to maintain information of different security levels within a single system, and to promptly and efficiently move information between levels under rigorous security controls, is essential to a system of this nature. The Air Surveillance scenario provides a natural and comprehensible example of this kind of system, although the assumptions upon which it is based are by their nature somewhat arbitrary.

COMPLETENESS

Each of the scenarios described here uses, and depends on, the major capabilities of the kernel, supervisor, and application level software on which they operate. The text editing scenario uses a flexible, general-purpose editor program to demonstrate the access control and multi-user support capability of a kernel-based system. Each feature of the editor is exercised during the scenario, in order to present a realistic and comprehensive illustration of the system's operation and use.

The Air Surveillance scenario is based on a much larger and more specialized set of application software. That software was designed to support a variety of multilevel secure air tracking and information downgrading simulations, with particular emphasis on features appropriate for multi-source correlation of tactical sensors. Because of time and reasonableness constraints, the scenario described here does not in fact utilize every key and every capability of the application software system. It does take full advantage of the system's major capabilities, those of storing, protecting, displaying and transferring multiple security levels of information in a pseudo-real-time environment. The development of alternative scenarios using the same system of application programs, but tailored to simulate other Air Force application areas, is not a technically demanding chore; the principal requirement is an understanding of the specific application of interest.

EFFECTIVENESS

These two types of scenarios are intended to provide an actual demonstration of the capability of realistic, kernel-based

application software systems, operating in the environment of multilevel security. User operations in each of these demonstrations is purely interpretive, via application software; in neither case is an on-line programming capability provided to the user. That capability appears to be the one which places the most stringent demands on the security kernel concept, since the user is allowed and expected to exercise every facet of the machine. However, the threat of undetected vulnerabilities in the outer layers of software makes the use of a security kernel essential even in a non-user-programmable system. It is perfectly possible to design and implement the application software in such a system to incorporate security controls; it is, however, extremely difficult to provide assurance that such security controls cannot be circumvented. The software used in the demonstrations was certainly not designed to incorporate any intentional security vulnerabilities, but it would be foolhardy to assert that no weaknesses or errors exist in either the user-level or system-level programs. Only the security kernel provides assurance that the demonstration systems provide the control of security that their application would require.

The protection provided by a secure system is not demonstrable in the usual sense. Examples of the system's refusal to allow accesses which would violate security cannot be taken as meaningful demonstrations of the system's actual security capabilities. The security of the system must be demonstrated in a formal and precise manner, rather than by exercising a few test cases. The verification of the PDP-11/45 security kernel's correctness is being developed under MITRE Project 572B; the kernel does provide proper protection for the demonstrations described here.

The scenario descriptions presented here are necessarily static in nature. Specific operation actions are described as followed by fixed system responses, followed by further specific operator actions, etc. In operation, both demonstration scenarios retain a degree of flexibility not conveyed by the static descriptions. The text editing demonstration starts with a specific text selection, but the operator is free to perform whatever accesses and alterations he chooses to exercise the system. Similarly, the Air Surveillance demonstration is driven by a predetermined sequence of track messages, but the operator can take a variety of actions, as he sees fit, within the capabilities of the system.

The demonstration scenarios described here have served their purpose by showing that the kernel-controlled PDP-11/45 can:

(1) support a structured data base system;

(2) protect classified information in the system from access by persons and processes not cleared or authorized need-to-know for that information; and

(3) implement a downgrading capability which is properly responsive to the judgment of a cleared and authorized downgrading officer, who is in complete control of the exact information downgraded.

SECTION VI

SUMMARY

This volume has described the two demonstrations which have been developed to show that the PDP-11/45 with security kernel mediation can:

(1) operate efficiently to support a data base system;

(2) properly protect classified information in the system from security compromise;

(3) effectively perform jobs to concurrently support the requirements of users with various clearances; and

(4) implement a secure downgrading facility suitable for supporting AF needs in a multi-source data correlation facility.

The two demonstrations and their associated scenarios are:

(1) the Text Editing scenario, that demonstrates that the system provides a capability for building and modifying a structured, multiple-security-level data base to serve users with different clearances and needs-to-know, while constraining each user to access or modify only that data for which he is specifically cleared and authorized;

(2) the Air Surveillance scenario, that provides a fictional situation of an Air Surveillance and Control system that must perform data correlation between compartmented and collateral track file data bases, and that provides a capability for precisely controlled temporary selective downgrading using cleared human intervention to support the correlation between the files for flight safety, while protecting against the possibility of security compromise.

The accomplishments and limitations of the demonstration have been assessed.

APPENDIX I

LISTING OF TEXT EDITING SCENARIO WITH SYSTEM RESPONSES[1]

USER #8

START 8 2 U 0 11

START ACCEPTED

MONITOR

$ LOAD EDITOR

EDITOR ENTERED

* F 0 4 2 8

* F SATIN-IV-SPEC SECTION-3.1 TEXT

* P 10 80 N

3.1 (U) SYSTEM SECURITY

SATIN IV SHALL BE SECURED IN A MANNER THAT WILL PROHIBIT UNAUTHORIZED ACCESS TO THE INFORMATION CONTAINED THEREIN. SATIN IV SYSTEM SECURITY CONTROLS SHALL INCLUDE SECURITY CONTROLS IN THE SYSTEM SEGMENTS DESCRIBED UNDER SECTION 3.1.2.

---

* F -1 SUB-1 TEXT

* P 10 90 N

3.1.1 (U) TRANSMISSION SYSTEM SEGMENT SECURITY CONTROLS

---

[1] System responses are underlined.

ALL SATIN IV TRANSMISSIONS LINKS SHALL BE SECURED IN A MANNER THAT WILL PROHIBIT UNAUTHORIZED ACCESS TO THE INFORMATION TRANSMITTED OVER THE LINK. FOR THOSE LINKS THAT CANNOT USE PROTECTED WIRELINE DISTRIBUTION SYSTEM (PWDS) TECHNIQUES, FULL PERIOD, LINK ENCRYPTION, GFP COMSEC EQUIPMENT SHALL BE EMPLOYED.

---

* F -2 SUB-5 TEXT

ERROR WITH FETCH OF BLOCK

CURRENT SUBSCRIPT LIST:

0

4

2

8

1

2

6

* F 0 4 2 8 SATIN-IV-SPEC

* F TITLE

ARE YOU CREATING A NEW BLOCK:

ENTER Y FOR YES OR N FOR NO - Y

WHICH CLASSIFICATION DO YOU WANT FOR NEW DIRECTORY

CLASS CODES: UNCLASSIFIED = U, CONFIDENTIAL = C,

SECRET = S, TOP SECRET = T - ENTER CODE - U

```
ENTER CATEGORY CODE - 0
* I 10 10 C
        10 COMPUTER SECURITY
        20 SATIN IV SPECIFICATION
        30 ƀƀ
        40.
* P 10 30
     10         COMPUTER SECURITY
     20    SATIN IV SPECIFICATION
     30
* F -1 SECTION-3.1 SUB-6 TEXT
* P 10 120
     10 3.1.6 (U) COMMUNICATIONS PROCESSOR SECURITY
     20
     30        SATIN IV COMMUNICATIONS PROCESSORS AND UTES SHALL BE
     40  DESIGNED AND IMPLEMENTED WITH EFFECTIVE INTERNAL ACCESS
     50  CONTROLS WHICH PREVENT MISROUTING OF MESSAGES THAT WOULD
     60  LEAD TO A POTENTIAL OR ACTUAL SECURITY COMPROMISE.  THE
     70  INTERNAL ACCESS CONTROLS SHALL PROVIDE USEFUL TOOLS FOR
     80  THE DEVELOPMENT OF SYSTEM INTEGRITY FOR SATIN IV; I.E., A
     90  HIGH PROBABILITY THAT SATIN IV WILL CORRECTLY PERFORM ITS
    100  REQUIRED OPERATIONAL CAPABILITY OF PROPERLY ROUTING
```

110 MESSAGES IN A PROMPT AND RELIABLE MANNER.

120

* CP

120

* T

* CP

0

* L /COMPROMISE/

60 LEAD TO A POTENTIAL OR ACTUAL SECURITY COMPROMISE. THE

* T

* R /CONTROL/MEASURE/6

50 MEASURES WHICH PREVENT MISROUTING OF MESSAGES THAT WOULD

70 INTERNAL ACCESS MEASURES SHALL PROVIDE USEFUL TOOLS FOR

NO MATCH

* P 10 120

10 3.1.6 (U) COMMUNICATIONS PROCESSOR SECURITY

20

30 SATIN IV COMMUNICATIONS PROCESSORS AND UTES SHALL BE

40 DESIGNED AND IMPLEMENTED WITH EFFECTIVE INTERNAL ACCESS

```
 50  MEASURES WHICH PREVENT MISROUTING OF MESSAGES THAT WOULD
 60  LEAD TO A POTENTIAL OR ACTUAL SECURITY COMPROMISE.  THE
 70  INTERNAL ACCESS MEASURES SHALL PROVIDE USEFUL TOOLS FOR
 80  THE DEVELOPMENT OF SYSTEM INTEGRITY FOR SATIN IV; I. E., A
 90  HIGH PROBABILITY THAT SATIN IV WILL CORRECTLY PERFORM ITS
100  REQUIRED OPERATIONAL CAPABILITY OF PROPERLY ROUTING
110  MESSAGES IN A PROMPT AND RELIABLE MANNER.
120
* T
* R /MEASURE/CONTROL/2
 50 CONTROLS WHICH PREVENT MISROUTING OF MESSAGES THAT WOULD
 70 INTERNAL ACCESS CONTROLS SHALL PROVIDE USEFUL TOOLS FOR
* X
EDITOR ENDED
MONITOR
$ HALT
(line feed)
START 8 2 S 0 11
START ACCEPTED
MONITOR
$ LOAD EDITOR
EDITOR ENTERED
```

```
* F 0 1 4

* IC 1

(Delta Data screen cleared)

↑FR 0 4 2 8 SATIN-IV-SPEC TITLE

↑P 10 20 N

↑FR -1 SECTION-3.1 TEXT

↑P 10 80 N

↑FR -1 SUB-2 TEXT

↑P 10 150 N

↑FR -2 SUB-4 TEXT

↑P 10 160 N

↑FR -2 SUB-5 TEXT

↑P 10 240 N

↑X

↑.

* P 1 11

      1 FR 0 4 2 8 SATIN-IV-SPEC TITLE

      2 P 10 30 N

      3 FR -1 SECTION-3.1 TEXT

      4 P 10 80 N

      5 FR -1 SUB-2 TEXT
```

```
   6 P 10 150 N
   7 FR -2 SUB-4 TEXT
   8 P 10 160 N
   9 FR -2 SUB-5 TEXT
  10 P 10 240 N
  11 X
* LP
* X
EDITOR ENDED
MONITOR
$ HALT
(line feed)
START 8 2 U 0 11
START ACCEPTED
MONITOR
$ LOAD UTILITY
FILE MANAGEMENT SYSTEM UTILITY - 3/10/75
#
```

USER #9

START 9 2 U 0 11

START ACCEPTED

MONITOR

$ LOAD EDITOR

EDITOR ENTERED

* F 0 4 2 8 SATIN-IV-SPEC

ERROR WITH FETCH OF BLOCK

CURRENT SUBSCRIPT LIST:

0

4

2

*

USER #8

CHANGE 0 4 2 W

1

0

4

2

LENGTH: 3

GIVE 8 W 9 2

1

USER #9

```
* F 0 4 2 8

* F SATIN-IV-SPEC SECTION-3.1 SUB-3 TEXT

* P 10 40

  10 3.1.3. (U) USER SECURITY CONTROL

  20

  30  EACH UTE SHALL BE SECURED IN A MANNER THAT WILL

  40  PROHIBIT UNAUTHORIZED ACCESS TO THE INFORMATION PROCESSED

*
```

APPENDIX II

SAMPLE TEXT EDITING PRINTOUT FROM LINE PRINTER AND DECWRITER

LINE PRINTER

PRINTING STARTED FOR PROCESS 4

(NEW PAGE ADVANCED ON LINE PRINTER)

COMPUTER SECURITY
SATIN IV SPECIFICATION

3.1 (U) SYSTEM SECURITY*

SATIN IV SHALL BE SECURED IN A MANNER THAT WILL PROHIBIT UNAUTHORIZED ACCESS TO THE INFORMATION CONTAINED THEREIN. SATIN IV SYSTEM SECURITY CONTROLS SHALL INCLUDE SECURITY CONTROLS IN THE SYSTEM SEGMENTS DESCRIBED UNDER SECTION 3.1.2.

3.1.2. (S) PROCESSOR SYSTEM SEGMENT SECURITY CONTROLS*

EACH COMMUNICATIONS PROCESSOR SHALL BE SECURED IN A MANNER THAT WILL PROHIBIT UNAUTHORIZED ACCESS TO THE INFORMATION PROCESSED THEREIN. SPECIFICALLY, EACH PROCESSOR CONNECTED TO AN INTERFACE OR UTE WHICH IS NOT AUTHORIZED TO RECEIVE TOP SECRET AND HAVE ACCESS TO SIOP/ESI AND SI/SAO INFORMATION SHALL INSURE THAT MESSAGE TRAFFIC MARKED AS CLASSIFIED ABOVE THE LEVEL AUTHORIZED FOR THE INTERFACE OR UTE OR IN A CATEGORY NOT AUTHORIZED FOR THAT INTERFACE OR UTE WILL NOT BE TRANSMITTED TO THAT INTERFACE OR UTE. IN ADDITION, EACH PROCESSOR SHALL INSURE THAT THE INTEGRITY OF THE MESSAGES IS MAINTAINED COMMENSURATE WITH ITS CONTENTS.

3.1.4. (S) THREATS TO SATIN IV COMMUNICATIONS PROCESSORS AND UTES*

THE BASIC ACTIVE THREAT TO SECURITY WITHIN THE COMMUNICATIONS PROCESSORS COMES FROM THE POSSIBILITY OF MALICIOUS SOFTWARE BEING INSERTED INTO THE OPERATING SYSTEM OR THE APPLICATIONS PROGRAMS. SUCH MALICIOUS SOFTWARE COULD TAKE DIRECT ACTIONS TO COMPROMISE MESSAGE SECURITY UNDER PREDETERMINED CONDITIONS (THIS IS KNOWN AS THE "TROJAN HORSE" THREAT), OR IT COULD TURN CONTROL OF THE PROCESSOR

*These markings are for illustrative purposes only. This material is unclassified.

OVER TO A SPECIFIC USER WHO HAD ENTERED A PRE-ARRANGED CHARACTER STRING (THIS IS KNOWN AS THE "TRAP-DOOR" THREAT). IN ADDITION TO THESE ACTIVE THREATS, THERE IS A RISK OF SECURITY COMPROMISES RESULTING FROM NON-MALICIOUS ERRORS IN THE OPERATING SYSTEM OF THE APPLICATIONS PROGRAMS.

3.1.5 (C) INTERFACE SECURITY*

EXTERNAL COMPUTER SYSTEMS THAT INTERFACE WITH SATIN IV COMMUNICATIONS PROCESSORS FALL INTO ONE OF TWO CLASSES -- THOSE WITH HUMAN REVIEW OF THE MESSAGES PASSING THROUGH THE INTERFACE AND THOSE WITHOUT. THOSE PASSING MESSAGES WITHOUT HUMAN REVIEW ARE CLASSED INTO TWO CATEGORIES, THOSE WITH CERTIFIED INTERNAL SECURITY CONTROLS AND THOSE WITHOUT. SYSTEMS WITH CERTIFIED CONTROLS SHALL BE INTERFACED SUCH THAT MESSAGES MAY BE EXCHANGED WITH THE SATIN IV SYSTEM USING A PROTOCOL THAT PROVIDES FOR LABELS WHICH INDICATE THE CLASSIFICATION AND CATEGORY FOR EACH MESSAGE, IMPLEMENTED SO THAT THE BASIC REQUIREMENTS FOR SATIN IV MESSAGE LABELS ARE MET. SYSTEMS WITHOUT CERTIFIED INTERNAL CONTROLS SHALL BE INTERFACED SUCH THAT ALL MESSAGES RECEIVED FROM THE SYSTEMS ARE TREATED AS IF UNMARKED. SATIN IV SHALL TREAT ANY MESSAGE RECEIVED FROM SUCH UNCERTIFIED SYSTEMS AS IF CLASSIFIED AT THE HIGHEST LEVEL THE EXTERNAL SYSTEM IS AUTHORIZED TO HANDLE AND AS IF IT WERE MARKED WITH THE MOST RESTRICTIVE SET OF CATEGORIES THE EXTERNAL SYSTEM IS AUTHORIZED TO PROCESS. SATIN IV MAY TRANSMIT ANY MESSAGE TO ANY EXTERNAL SYSTEM WHICH IT IS AUTHORIZED TO RECEIVE.

(NEW PAGE ADVANCED ON LINE PRINTER)

PRINTING ENDED FOR PROCESS 4

<u>DECwriter</u>

OUTPUT: PROCESS 4, USER 8 2 3 0

ACKNOWLEDGE CLASS AND CAT: 3 0

OUTPUT ENDED

*These markings are for illustrative purposes only. This material is unclassified.

APPENDIX III

TRACK MESSAGE INPUT TIME LINES

This appendix presents a printout of each of the time ordered input track message lists which are used in the Southwest and European scenario demonstrations. Each printout shows the track messages to be stored in the appropriate track message file prior to the beginning of the demonstration. A description of the message formats is contained in Section III of Volume IV of this report.

HIGH TRACK MESSAGE INPUTS

FOR SOUTHWEST SCENARIO

TIME	TRN	POS	HDG	SPD	ALT	TYPE	
090000	BQ12	PD4803	301DG	150KT	6KF	NEW	SORC=X TID=ASPEC SIZ=1AC
090200	BQ12	PD4010	280DG	200KT	10KF	UPD	QLTY=XCLT
090200	HA12	PC4849	220DG	130KT	7KF	NEW	SORC=Z TID=GEN SIZ=1AC
090300	HA12	PC4647				UPD	QLTY=XCLT
090400	BQ12	PD3012	279DG	320KT	15KF	UPD	
090400	BQ13	PD4106	280DG	210KT	13KF	NEW	SORC=X TID=ASPEC SIZ=2AC
090400	HA13	PC5556	350DG	150KT	6KF	NEW	SORC=Z TID=TSTAF SIZ=1AC
090400	HA12	PC4445	220DG	150KT	8KF	UPD	SORC=Z SIZ=1AC QLTY=XCLT
090500	BQ13	PD3606	285DG	225KT	13KF	UPD	
090600	BQ13	PD3107	290DG	265KT	14KF	UPD	
090700	BQ12	PD1215	280DG	380KT	18KF	UPD	
090700	BQ13	PD2508	280DG	300KT	15KF	UPD	QLTY=XCLT
090700	HA13	PD5410	5DG	260KT	10KF	UPD	QLTY=XCLT
090700	HA12	PC3839	200DG	180KT	11KF	UPD	
090800	BQ13	PD1908		320KT	16KF	UPD	
090800	HA13	PD5615		360KT	15KF	UPD	
090900	BQ13	PD1509			18KF	UPD	
090900	HA13	PD5623		480KT		UPD	
091000	BQ12	ND5119		390KT	22KF	UPD	
091000	BQ13	PD1110			23KF	UPD	
091000	HA13	QD0133	10DG	600KT	20KF	UPD	
091000	HA12	PC3826	210DG	220KT	13KF	UPD	
091100	HA12	PC3621				UPD	
091100	BQ13	PD0511				UPD	SIZ=1AC
091100	HA13	QD0146	345DG	650KT	22KF	UPD	
091100	BQ14	PD0309	275DG	380KT	22KF	NEW	SORC=X TID=ASPEC SIZ=1AC

HIGH TRACK MESSAGE INPUTS FOR

SOUTHWEST SCENARIO (concluded)

TIME	TRN	POS	HDG	SPD	ALT	TYPE
091200	BQ13	PD0111	285DG			UPD
091200	HA13	PE5600	310DG	680KT	28KF	UPD
091200	HA12	PC3217				UPD
091200	BQ14	ND5509	320DG			UPD
091300	HA12	PC2515	215DG	230KT	14KF	UPD
091300	BQ14	ND4710				UPD
091300	BQ13	ND5512				UPD
091300	HA13	PE4006	264DG	720KT	32KF	UPD
091400	BQ14	ND4112	285DG			UPD
091400	HA12	PC2212	245DG	240KT		UPD
091400	BQ12	ND2026	285DG	390KT		UPD
091400	BQ13	ND5013	290DG			UPD
091400	HA13	PD2756	200DG	760KT	30KF	UPD
091500	BQ14	ND3918	305DG			UPD
091500	BQ13	ND4614	295DG			UPD
091500	HA13	PD3242	160DG	770KT	28KF	UPD
091600	HA12	PC1006	255DG	245KT	15KF	UPD
091600	BQ13	ND4317	325DG			UPD
091600	HA13	PD4329	145DG	900KT	25KF	UPD
091600	BQ14	ND3825	350DG	400KT		UPD
091700	BQ13	ND4121	340DG			UPD
091700	HA13	PD5715	145DG	920KT	15KF	UPD
091700	BQ14	ND3833	ODG			UPD
091800	BQ12	MD4933	300DG	400KT		UPD
091800	HA12	PC0003	270DG	250KT	16KF	UPD
091800	BQ13	ND4228	2DG	400KT		UPD
091800	HA13	QD0500	170DG	850KT	15KF	UPD
091900	BQ12	MD2852	310DG			UPD
091900	BQ13	ND4126	10DG			UPD
091900	HA13	QC0442	225DG	680KT		UPD
092000	HA12	NC5102	272DG	260KT		UPD
092000	BQ13	ND4539				UPD
092000	HA13	PC5238	266DG	640KT		UPD

LOW TRACK MESSAGE INPUTS

FOR SOUTHWEST SCENARIO

TIME	TRN	POS	HDG	SPD	ALT	TYPE	
090000	MD12	MC4110	102DG	420KT	36KF	NEW	SORC=A TID=COMLP SIZ=1AC
090000	PB23	PC0240	340DG	220KT	19KF	NEW	SORC=C TID=GEN SIZ=1AC QLTY=FAIR
090200	MD12	MC5702	105DG		34KF	UPD	QLTY=XCLT
090200	PB23	PC0043	340DG	220KT	19KF	UPD	
090400	MD12	NB1158				UPD	
090400	PB23	NC5548	335DG	220KT	21KF	UPD	
090400	AG25	QF2502	185DG	500KT	35KF	NEW	SORC=E TID=KILO SIZ=1AC
090500	AG25	QE2452	181DG			UPD	QLTY=XCLT
090600	PB23	NC5554			23KF	UPD	
090600	AG25	QE2342	170DG			UPD	
090700	MD12	NB2754	104DG	420KT	33KF	UPD	
090700	AG25	QE2632				UPD	
090800	PB23	NC5259				UPD	
090800	AG25	QE2823	160DG			UPD	
090900	AG25	QE3213	152DG			UPD	
090900	PB23	ND5103	340DG			UPD	
091000	MD12	NB5054	104DG	420KT	31KF	UPD	
091000	PB23	ND5005	340DG	220KT	26KF	UPD	QLTY=GOOD
091000	AG25	QE3801	155DG			UPD	
091100	MD12	NB5755	80DG	420KT	31KF	UPD	
091100	PB23	NB4708	310DG	200KT	27KF	UPD	
091100	AG25	QD3954	170DG			UPD	
091200	MD12	PB0558	88DG	400KT		UPD	
091200	PB23	ND4408	271DG	230KT		UPD	
091200	AG25	QD4244			32KF	UPD	
091300	NC54	PC2515	215DG	230KT	14KF	NEW	TID=GEN SIZ=1AC QLTY=XCLT SORC=D
091300	PB23	ND4008				UPD	
091300	MD12	PB1159				UPD	
091300	AG25	QD4435	172DG		30KF	UPD	
091400	NC54	PC2212	245DG	240KT		UPD	
091400	MD12	PC1700	91DG	380KT	28KF	UPD	QLTY=GOOD
091400	PB23	ND3608	271DG	200KT	27KF	UPD	
091400	AG25	QD4725	181DG		25KF	UPD	
091500	PB23	ND3208	271DG	210KT		UPD	
091500	AG25	QD4714			20KF	UPD	
091500	MD12	PC2600	93DG			UPD	

LOW TRACK MESSAGE INPUTS FOR

SOUTHWEST SCENARIO (concluded)

TIME	TRN	POS	HDG	SPD	ALT	TYPE	
091600	MD12	PD3258	100DG	370KT	26KF	UPD	
091600	AG25	QD4707	185DG	400KT	18KF	UPD	
091600	NC54	PC1006	255DG	245KT	15KF	UPD	
091600	PB23	ND2709	290DG			UPD	
091700	PB23	ND2212	310DG			UPD	
091700	AG25	QC4559			17KF	UPD	
091800	MD12	PB4350	130DG	360KT	24KF	UPD	QLTY=GOOD
091800	PB23	ND2016	345DG	200KT	25KF	UPD	
091800	AG25	QC4351	200DG	380KT	14KF	UPD	
091800	NC54	PC0003	270DG	250KT	16KF	UPD	
091900	MD12	PB4748		340KT	22KF	UPD	QLTY=GOOD
091900	PB23	ND2122	5DG	240KT		UPD	
091900	AG25	QC4042	240DG	340KT	12KF	UPD	QLTY=XCLT
092000	MD12	PB5145				UPD	QLTY=FAIR
092000	PB23	ND2726	40DG	220KT	25KF	UPD	
092000	AG25	QC3734	200DG		10KF	UPD	
092000	NC54	NC5102	272DG	260KT		UPD	

HIGH TRACK MESSAGE INPUTS

FOR EUROPEAN SCENARIO

TIME	TRN	POS	HDG	SPD	ALT	TYPE		
070200	R001	AJ3621	271DG	720KT	22KF	NEW	TID=PE	SIZ=3AC SORC=X
070300	R002	PJ1836	271DG	240KT	02KF	NEW	TID-JFSHB	SIZE=3AC SORC=Y
070400	R001				13KF	UPD		
070400	R002	PJ1036	281DG	600KT	06KF	UPD		
070500	R002	NJ5238	288DG		05KF	UPD		
070600	R001				08KF	UPD		
070600	R002				02KF	UPD		
070700	R002	NJ1744	277DG			UPD		
070800	R001	PJ2622	280DG		05KF	UPD	TID=BLDR	SIZE-3AC SORC=y
070900	R001				02KF	UPD		
071000	R002					DEL		
071200	R001	NJ0231	270DG		01KF	UPD	QLTY=GOOD	
071400	R001					DEL		
071700	*R025*	*AG3555*	*272DG*	820KT	*18KF*	*NEW*	TID=BLDR	SIZE=MANY SORC=Z
072000	R025		284DG	900KT	15KF	UPD	QLTY=GOOD	

LOW TRACK MESSAGE INPUTS

FOR EUROPEAN SCENARIO

TIME	TRN	POS	HDG	SPD	ALT	TYPE			
070000	KH20	KH3628	254DG	290KT	09KF	NEW	TID=CMLP	SIZ=1AC	SORC=B
070000	BP01	KF4756	0DG	610KT	33KF	NEW	TID=INTF	SIZ=3AC	SORC=C
070000	BP02	KG3710	200DG	620KT	35KF	NEW	TID=INTF	SIZ=3AC	SORC=C
070000	RP01	MG0135	33DG	500KT	20KF	NEW	TID=FLOGC	SIZ=2AC	SORC=A
070100	KH20	KH2727		395KT	11KF	UPD	QLTY=GOOD		
070100	BP02	KG3100	216DG			UPD	QLTY=GOOD		
070200	KH20	KH1325		405KT	13KF	UPD			
070200	BP01	KG4718	23DG			UPD			
070200	BP02	KF1852	153DG	580KT	35KF	UPD			
070300	BP01	KG5428	40DG			UPD			
070300	BP02	KF2742	70DG	600KT	35KF	UPD			
070400	BP02	KF4446	10DG		35KF	UPD			
070400	RP02	NJ1058	180DG	500KT	19KF	NEW	TID=FLOGC	SIZ=3AC	SORC=H
070500	KH20				16KF	UPD			
070500	BP01	LG1944	7DG			UPD			
070500	BP02	KF4957	0DG	600KT	35KF	UPD			
070500	RP01	MH4410	2DG			UPD			
070500	RP02	NJ1050	195DG			UPD			
070600	BP01			660KT		UPD			
070700	BP01			720KT		UPD			
070700	BP02	KG4918	31DG			UPD			
070700	RP02	NJ0234	182DG			UPD			
070800	KH20					DEL			
070800	BP01		2DG	800KT		UPD			
070900	BP01			920KT		UPD			
070900	BP02	LG0834	2DG	700KT		UPD			
070900	MJ02	MJ4047	288DG	600KT	01KF	NEW	TID=PE	SIZ=3AC	SORC=H
071000	BP01			1200KT		UPD			
071000	RP01	MH4853	2DG			UPD			
071100	BP01			1250KT	14KF	UPD			
071100	BP03	JH1828	84DG	600KT	20KF	NEW	TID=INTF	SIZ=MANY	SORC=B
071100	MJ02	MJ0350	254DG			UPD			
071200	BP01	LJ3024	350DG	920KT	10KF	UPD			
071200	BP02	LH2112	17DG	900KT	08KF	UPD			
071200	RP02	NH0052	185DG			UPD			
071300	BP01	LJ2641	278DG	890KT	02KF	UPD			
071300	BP02			920KT	04KF	UPD			
071300	BP03	JH5532		705KT		UPD			
071300	MJ03	MJ4031	270DG	700KT	01KF	NEW	TID=PE	SIZ=3AC	
071400	RP01		358DG			UPD			
071400	LH20					DEL			
071400	BP01	KJ5643	237DG	820KT		UPD			
071400	BP02			1380KT		UPD			
071400	MJ02					DEL			

LOW TRACK MESSAGE INPUTS FOR

EUROPEAN SCENARIO (concluded)

TIME	TRN	POS	KDG	SPD	ALT	TYPE		
071500	BP02	LJ3603	356DG	1200KT		UPD		
071500	BP01	KJ3535	240DG	800KT	05KF	UPD		
071500	BP03	KH3933	112DG	700KT		UPD	SIZ-2AC	TID=INTF
071500	BP04	KH4037	75DG	705KT	20KF	NEW	SIZ=3AC	TID=INTF
071600	BP02	LJ3127	292DG	920KT	02KF	UPD		
071600	BP03	KH5928	156DG	660KT		UPD		
071600	BP04	LH0140	48DG	680KT		UPD		
071700	BP02	LJ1231	238DG	820KT	02KF	UPD		
071700	BP01				10KF	UPD		
071700	BP03	LH0706	192DG			UPD		
071700	RP02	MH5510	186DG			UPD		
071700	MJ03					DEL		
071700	BP04	LH1747	14DG			UPD		
071800	BP02	KJ5023	235DG	600KT	04KF	UPD		
071800	RP01					DEL		
071900	BP02				07KF	UPD		
071900	RP02	MG5253			22KF	UPD		
072200	BP01					DEL		
072200	RP02					DEL		